Office of the Governor
State Chief Information Officer

SECURITY

Chapter 8 – Developing and Maintaining In-House Software

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: G.S. 147-33.110

Section 01 Controlling Software Code

080101 Managing Operational Program Libraries

Purpose: To protect agency software by restricting access to operational program libraries.

STANDARD

Agencies shall restrict access to operating system and operational or production application software/program libraries to designated staff only.

GUIDELINES

Managing the directories or locations used to store production (live) software and configuration files is an integral part of risk management.

To prevent the corruption of information systems or the disruption of business operations, agencies should ensure that their program libraries are adequately protected. Appropriate technical controls and procedures for protecting program libraries should be designed to prevent unauthorized use (intentional and unintentional).

Agencies should consider processes, controls or best practices in the following areas:

- Updating of libraries.
- Restricting library content to executable code.
- Version control for each application.
- Tying system documentation updates to application software library updates.
- Audit logs that track all:
  - Accesses to libraries.
  - Change requests.

- Copying and use of operational information.
- Updates posted to libraries.

- Defining job responsibilities and establishing authority levels for:
  - Program librarian(s).
  - Personnel authorized to make or submit changes to program libraries. (Developers should not be permitted to promote their own code into libraries.)
- Rollback procedures designed to recover to old, stable versions of programs.

ISO 17799: 2005 References
12.4.1 Control of operational software
12.5.1 Change control procedures

080102 Managing Program Source Libraries

Purpose: To protect the integrity of business operations software by managing source code libraries.

STANDARD

Agencies shall manage access to source code or source program libraries, limiting access to authorized individuals.

- Production source code and development source code libraries must always be kept separate.
- Agencies shall implement a combination of technical access controls and robust procedures to restrict access to source program libraries to authorized personnel only.

RELATED INFORMATION

Standard 080104	Controlling Program Listings
Standard 080105	Controlling Program Source Libraries
Standard 080106	Controlling Old Versions of Programs

ISO 17799: 2005 References
12.4.3 Access control to program source code

080103 Controlling Software Code during Software Development

Purpose: To protect information systems from corruption by controlling software change.

STANDARD

When developing or modifying software, agencies shall establish a change control management process that implements the following rules:

- Authorization is required to initiate or make changes to software.

- Change control procedures that govern changes to system software are defined and utilized.
- All changes must pass acceptance testing prior to moving changed code into a live or production environment.
- Senior management may authorize emergency exceptions to this standard only to avoid imminent failure of business operations.

RELATED INFORMATION

Standard 080104	Controlling Program Listings
Standard 080105	Controlling Program Source Libraries
Standard 080106	Controlling Old Versions of Programs

ISO 17799: 2005 References
12.5.1 Change control procedures
12.5.3 Restrictions on changes to software packages

080104 Controlling Program Listings

Purpose: To protect the integrity of software by controlling program listings.

STANDARD

Agencies shall maintain and control current electronic and hard copy listings of application/program source code that runs on agency systems.

GUIDELINES

Program listings are the primary tool for identifying system problems. Loss or unavailability of a listing could delay problem identification and resolution, the consequence of which could put agency services at risk.

Unauthorized access to program listings compromises system security by making exact logic and system routines available for exploitation.

ISO 17799: 2005 References
10.7.4 Security of system documentation
12.4.3 Access control of program source code

080105 Controlling Program Source Libraries

Purpose: To protect the integrity of business operations software by controlling source code libraries.

STANDARD

Agencies shall exercise strict control over program source libraries by implementing the following:

- Formal change control procedures.
- Comprehensive audit trails.

- Monitoring.

GUIDELINES

Formal change control procedures can aid in the investigation of changes made to agency program source libraries. Agencies should establish a regular review of audit reports and event logs to ensure that incidents that have potentially compromised program source libraries are detected.

RELATED INFORMATION

Standard 080102	Managing Program Source Libraries
Standard 080104	Controlling Program Listings

ISO 17799: 2005 References
12.4.3 Access control to program source code
12.5.1 Change control procedures

080106 Controlling Old Versions of Programs

Purpose: To protect system integrity with software version control.

STANDARD

Agencies shall control old versions of programs by establishing the following:

- Comprehensive procedures for auditing removals or updates to program libraries.
- Formal change control procedures to process the application code used to write programs within agency systems when that code has been superseded or discontinued.

GUIDELINES

Information security issues to be considered when implementing an agency policy in regard to old versions of programs include the following:

- When application code within agency systems has been superseded or discontinued, agencies should be prepared to roll back or access the superseded or discontinued code if required, because decommissioned code must often be resurrected if major bugs are found in the newer version.
- Version control is essential because there is a real danger of losing the latest program enhancements or of causing the failure of other systems that depend on recently added features if an older version of a program is confused with a newer version.

ISO 17799: 2005 References
12.4.1 Control of operational software
12.5.1 Change control procedures

Section 02 Software Development

080201 Software Development

Purpose: To protect production/operational software during all phases of the development process.

STANDARD

Each agency shall follow and manage a formal development process when it develops software. Safeguards shall include the following:

- A formal software development process that is managed by a project office/team.
- A combination of appropriate:
  - Technical access controls.
  - Restricted privilege allocations.
  - Robust procedures.

GUIDELINES

Agencies should address the following information security issues when updating or formalizing development processes:

- Potential compromise to production systems.
- The threat of insertion of malicious code within software.
- Disruption of live operations.
- Confidentiality, criticality and value of the systems and data to the agency and public.

RELATED INFORMATION

Standard 010102 Labelling Classified Information

ISO 17799: 2005 References

10.1.4 Separation of development, test, and operational facilities
12.1.1 Security requirements analysis and specifications
12.5.1 Change control procedures

080202 Making Emergency Amendments to Software

Purpose: To protect production software during emergency modifications

STANDARD

Agency personnel must fully justify their requests for emergency modifications to software and must obtain senior management authorization.

Agency personnel making emergency modifications must not deviate from the agency's change control procedures.

GUIDELINES

Each agency should establish an emergency procedure that personnel agree to follow if it becomes necessary to amend the live software environment quickly. The procedure should include management approval.

When developing emergency change control procedures, agencies should consider how these procedures will deviate from normal everyday change control procedures and best practices in the following areas:

- Updating of libraries.
- Restricting library content.
- Version control for each application.
- Tying program documentation updates to source code updates.
- Audit logs that track all:
  - Accesses to libraries.
  - Change requests.
  - Copying and use of source code.
  - Updates posted to libraries.
- Predefined job responsibilities/restrictions and establishment of authority levels that have been agreed to for:
  - Program librarian(s).
  - Developers.
  - Other IT staff.
- Personnel authorized to make or submit changes to the source library. (A program librarian should be appointed for each major application to control check-in/check-out.)
- Rollback procedures designed to recover to old, stable versions of programs.

RELATED INFORMATION

Standard 030209	Scheduling System Operations
Standard 030210	Scheduling Changes to Routine System Operations
Standard 030504	Permitting Emergency Data Amendment
Standard 080205	Managing Change Control Procedures

ISO 17799: 2005 References
12.5.1 Change control procedures

080203 Establishing Ownership for System Enhancements

Purpose: To protect systems by defining responsibilities and authority levels required for system change.

STANDARD

Agencies shall establish custodians for each system who will have responsibility for all system enhancements.

- All proposed system enhancements must be driven by the business needs of the agency and supported by a business case that has both user and management acceptance.
- Ownership for any such system enhancements ultimately lies with the system custodian and requires his/her commitment and personal involvement.

GUIDELINES

Allocation of information security responsibilities should be an integral part of each agency's information security program. Information security policy and job descriptions should provide general guidance on the various security roles and responsibilities within the agency. However, in the case of individual systems, the system custodian and a designated alternate manager should have more detailed guidelines governing enhancements to the system(s) for which they are ultimately responsible.

Agencies should consider the following areas when they are defining security job responsibilities for system custodians and other managers with focused security positions (e.g., security analysts and business continuity planners):

- Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible.
- Clearly defining and documenting the agreed-upon authorization levels that the position holder will have to make enhancements, modify source code, promote updated code, etc.
- Documenting the following for each asset:
  - Management's assignment of system responsibility to a specific manager/custodian.
  - Manager/custodian acceptance of responsibility for the system.
  - Detailed description of manager/custodian responsibilities.

ISO 17799: 2005 References
6.1.3 Allocation of Information Security responsibilities

080204 Justifying New System Development

Purpose: To require business case justification of custom system development projects.

STANDARD

When proposing the development of custom software, agencies shall make a strong business case that (1) supports the rationale for not enhancing current systems, (2) demonstrates the inadequacies of packaged solutions, and (3) justifies the creation of custom software.

Agencies shall consider custom software development only when the following conditions are met:

- A strong business case demonstrates that business requirements can be met only with the proposed software.
- Existing software cannot be economically updated to fulfill these business requirements.
- No suitable packaged solution can be found.
- The development is supported by agency management.
- The agency has adequate resources to support the estimated project timeline.
- The agency can support and maintain the product during its required lifetime.

GUIDELINES

Developing a system to meet a business need is a major decision that frequently carries significant risk.

Agencies should consider the following issues when weighing the decision to outsource a major system development effort:

- High risk of failure—Signing a contract with a vendor for outsourced development can be high risk and may pose a substantial risk to the agency.
- Senior management support and financial backing—When projects last more than 12 months, there is an increased potential for a reduction in both commitment and financial support that could have an impact not only on the project but on business operations as well.

ISO 17799: 2005 References
12.1.1 Security requirements analysis and specifications

080205 Managing Change Control Procedures

Purpose: To safeguard production systems during modification

STANDARD

Each agency shall manage changes to its systems and application programs to protect the systems and programs from failure as well as security breaches.

Adequate management of system change control processes shall require the following:

- Enforcement of formal change control procedures.
- Proper authorization and approvals at all levels.
- Successful testing of updates and new programs prior to their being moved into a live environment.
- Updates addressing significant security vulnerabilities shall be prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.

- Whenever an update is implemented, the application system the update affects shall be tested to ensure that business operations and security controls perform as expected.

GUIDELINES

Managing change control procedures is an integral part of risk management.

Each agency should enforce strict change control procedures because healthy application software fundamentally affects the agency's ability to do its work and deliver services. Inadequate or poorly managed change control procedures can result in compromises and failures not only in the operational system being modified, but also in other systems that are dependent on the new functionality provided by the updated system.

Appropriate technical controls and procedures for protecting program and source libraries should be designed to prevent unauthorized use. Loss of source code could make it difficult or impossible for an agency to maintain its systems, and unauthorized modification of programs could result in system failure or malicious damage.

When possible, agencies should integrate application change control and operational change control procedures. This effort should include the following processes, controls, and best practices:

- Controls and approval levels for updating libraries.
- Requiring formal agreement and approval for any changes.
- Restricting library content.
- Restricting programmers' access to only those parts of the system necessary for their work.
- Version control for each application.
- Tying program documentation updates to source code updates.
- Audit logs that track all:
  - Accesses to libraries.
  - Change requests.
  - Copying and use of source code.
  - Updates posted to libraries.
- Defining job responsibilities/restrictions and establishing authority levels for:
  - Program librarian(s).
  - Developers (i.e., should neither test their own code nor promote it into production).
  - Other IT staff.
- Personnel authorized to make or submit changes to the source library (i.e., a program librarian should be appointed for each major application to control check-in/check-out).
- Rollback procedures designed to recover to old, stable version of programs.

RELATED INFORMATION

Standard 040201	Applying Patches to Software
Standard 080101	Managing Operational Program Libraries
Standard 080102	Managing Program Source Libraries
Standard 080103	Controlling Software Code during Software Development
Standard 080104	Controlling Program Listings
Standard 080105	Controlling Program Source Libraries
Standard 080106	Controlling Old Versions of Programs
Standard 080201	Software Development
Standard 080202	Making Emergency Amendments to Software
Standard 080203	Establishing Ownership for System Enhancements
Standard 080204	Justifying New System Development
Standard 080206	Separating System Development and Operations
Standard 080301	Controlling Test Environments
Standard 080302	Using Live Data for Testing
Standard 080303	Testing Software before Transferring to a Live Environment
Standard 080304	Capacity Planning and Testing of New Systems
Standard 080305	Parallel Running
Standard 080306	Training on New Systems
Standard 080401	Documenting New and Enhanced Systems
Standard 080501	Acquiring Vendor-Developed Software

ISO 17799: 2005 Reference
12.5.1 Change control procedures

080206 Separating System Development and Operations

Purpose: To reduce the risk of agency system misuse and fraud by segregation of duties

STANDARD

Agency management must ensure that there is proper segregation of duties to reduce the risk of agency system misuse and fraud.

- System administration and system auditing shall be performed by different personnel.
- System development and system change management shall be performed by different personnel.
- System operations and system security administration shall be performed by different personnel.

Insofar as is technically possible, security administration and security audit shall be performed by different personnel.

Administrators of multi-user system must have at least two user IDs. One of these user IDs must provide privileged access, with all activities logged; the other must be a normal user ID for performing the day-to-day work of an ordinary user.

GUIDELINES

Separation of duties is an integral part of a successful information security program that reduces the risk of accidental or deliberate system misuse. Separation of duties reduces opportunities for unauthorized modification or misuse of information by segregating the management and execution of certain duties or areas of responsibility. Although smaller agencies without the manpower to staff separate sections or groups will find this method of control more challenging to implement, the principle should be applied to the extent possible.

Agencies should consider taking the following actions in regard to information security issues when implementing a separation-of-duties policy:

- When separation of duties is difficult, consider other controls such as:
  - Monitoring of activities.
  - Audit trails.
  - Management supervision.
- Keep the responsibility for security audit separate from other audit powers.
- Identify and segregate activities that require collusion to defraud (e.g., exercising a purchase order and verifying receipt of goods).
  - Consider dual control in instances in which collusion might result in the agency's being defrauded.
- Prohibit development staffs (who have powerful privileges in the development environment) from extending their administrative privileges to the operational environment.

ISO 17799: 2005 References
10.1.3 Segregation of duties
10.1.4 Separation of development, test, and operational facilities

---

Section 03 Testing & Training

080301 Controlling Test Environments

Purpose: To protect agency systems during development and modification.

STANDARD

Agencies shall ensure that all changes to programs are properly authorized and tested in a test environment before the programs are moved into an operational environment.

RELATED INFORMATION

Standard 080302 Using Live Data for Testing

Standard 080303 Testing Software before Transferring to a Live Environment

ISO 17799: 2005 References
10.3.2 System acceptance
12.5.1 Change control procedures

080302 Using Live Data for Testing

Purpose: To protect the integrity and confidentiality of data during system development and testing.

STANDARD

Agencies shall permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions.

If production data is used for testing, the following controls must be met:

- Testing of production data shall take place only on non-live, non-production systems.
- Adequate controls for the security of the data are in place.
- The test shall observe and maintain the confidentiality conditions established by the agency from which the data is obtained.

RELATED INFORMATION

Standard 010103 Storing and Handling Classified Information

ISO 17799: 2005 References
12.4.2 Protection of system test data

080303 Testing Software before Transferring to a Live Environment

Purpose: To protect agency systems by testing software prior to transferring it to the production environment.

STANDARD

To maintain the integrity of agency information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.

RELATED INFORMATION

Standard 080301	Controlling Test Environments
Standard 080302	Using Live Data for Testing

ISO 17799: 2005 References
10.3.2 System acceptance
12.5.1 Change control procedures

080304 Capacity Planning and Testing of New Systems

Purpose: To safeguard new system investments by projecting capacity demands and conducting load acceptance testing.

STANDARD

New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the agency. To understand current specifications, agencies shall establish a baseline of current operational systems, including peak loads and stress levels and power, bandwidth and storage requirements.

Agencies must also test to demonstrate that the new system's performance meets or exceeds the agency's documented technical requirements and business needs.

GUIDELINES

Agency capacity plans should consider new business, security and system requirements and any trends in the agency's information processing.

The agency's system-testing process should verify that new or amended systems have:

- Sufficient capabilities to process the expected transaction volumes (actual and peak).
- Acceptable performance and resilience.
- Reasonable scalability for growth of system.

RELATED INFORMATION

Standard 080301	Controlling Test Environments

ISO 17799: 2005 References
10.3.1 Capacity management
10.3.2 System acceptance

080305 Parallel Running

Purpose: To safely demonstrate the reliability and capability of new or updated systems.

STANDARD

If agencies test new or updated applications by running parallel tests, the agencies shall incorporate a period of parallel processing into system-testing procedures that demonstrates that the new or updated system performs as expected and does not adversely affect existing systems, particularly those systems that depend on the new or updated system's functionality.

GUIDELINES

Agencies should use parallel processing as the final stage of acceptance testing and should consider the following issues and controls when developing acceptance criteria and acceptance test plans for the parallel testing of new or updated systems:

- Capacity requirements—both for performance and for the computer hardware needed.
- Error response—recovery and restart procedures and contingency plans.
- Routine operating procedures—prepared and tested according to defined agency standards.
- Security controls—agreed to and put in place.
- Manual procedures—effective and available where feasible and appropriate.
- Business continuity—meets the requirements defined in the agency's business continuity plan.
- Impact on production environment—able to demonstrate that installation of new system will not adversely affect agency's current production systems (particularly at peak processing times).
- Training—of operators, administrators and users of the new or updated system.

RELATED INFORMATION

Standard 080301	Controlling Test Environments
Standard 080303	Testing Software before Transferring to a Live Environment

ISO 17799: 2005 References
10.3.2 System acceptance
12.5.1 Change control procedures

080306 Training in New Systems

Purpose: To ensure that personnel are adequately trained on new and updated systems.

STANDARD

Agencies shall provide training to users and technical staff in the operation and security of all new and updated systems.

GUIDELINES

Agencies should consider the following issues and training requirements when developing plans for training on new and updated systems:

- When administrative training is inadequate, small problems can unnecessarily escalate as a result of lack of knowledge of new functions or security controls.
- When user training is inadequate, work production often drops because of frustration or because of adjustments that must be made as users learn how to use the new system.
- Changes in information security processes, features and controls are inherent in new systems.

RELATED INFORMATION

Standard 080301 Controlling Test Environments

ISO 17799: 2005 References
8.2.2 Information security awareness, education, and training

Section 04 Documentation

080401 Documenting New and Enhanced Systems

Purpose: To protect information technology assets by maintaining comprehensive system documentation.

STANDARD

Whether the system is developed or updated by in-house staff or by a third-party vendor, agencies shall ensure that each new or updated system includes adequate system documentation.

Agencies shall create, manage and secure system documentation libraries or data stores that are available at all times but shall restrict access to authorized personnel only.

Agencies shall ensure that system documentation is readily available to support the staff responsible for operating, securing and maintaining new and updated systems.

GUIDELINES

Agencies should consider the following information security issues as they define their system documentation management strategies:

- A lack of adequate documentation, whether because the documentation is missing, out of date, or simply unavailable, can:

- Greatly increase the risk of a serious incident.
- Compromise performance of routine maintenance, especially as the complexity of the system increases.
- Increase the likelihood that errors and omissions will slip through peer reviews of source code into system testing and perhaps beyond into user acceptance testing.

- System documentation should be a required component of the system's inventory of assets (along with the physical and software assets that constitute the system).
- System documentation should be protected from unauthorized access by keeping it stored securely and by utilizing an access list limited to a small number of staff, all of whom have been authorized by the system custodian.
- A copy of system documentation should be maintained for disaster recovery and business continuity and stored off site.

ISO 17799: 2005 References
7.1.1 Inventory of assets
10.7.4 Security of system documentation

Section 05 Other Software Development

080501 Acquiring Vendor Developed Software

Purpose: To maximize the utility of vendor-developed software

STANDARD

Agencies shall comply with State purchasing and contracting laws, rules and policies when negotiating software development contracts with third-party developers. All contracts with vendors for software development must meet the agency's functional requirements specification and offer appropriate product support:

Agencies shall initiate formal contracts defining third-party access to the organization's information-processing facilities. Such contracts should include or refer to all security requirements and expected performance and support levels to ensure that there is no misunderstanding between the agency and the vendor.

- Agencies will find a detailed listing of the security requirements, terms and conditions that should be considered for inclusion in third-party contracts in ISO 17799, §4.2.2.

ISO 17799: 2005 References
6.2.3 Addressing security in third party agreements

HISTORY

State CIO Approval: April 17, 2006

Original Issue Date: April 17, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
There are no old security policies or standards that correspond to this chapter	